# **Cybersicherheit in Erneuerbaren Energieanlagen** Angriffserkennung nach NIS2 umsetzen

NIS2-COMPLIANCE IN DER OT SICHERSTELLEN

SCHWACHSTELLEN UND SICHERHEITSVORFÄLLE IN DER OT ERKENNEN

FACHKRÄFTEMANGEL IN DER OT-SICHERHEIT ÜBERBRÜCKEN

# Executive Summary

Erneuerbare Energien werden immer stärker zum entscheidenden Rückgrat für die deutsche Stromversorgung. Im Jahr 2023 wurden in Deutschland 139 TWh aus Windkraft, 53,5 TWh aus Photovoltaik und 18,8 TWh aus Wasserkraft erzeugt. Das entspricht bereits heute einem Anteil von über 40 % am gesamten Strommix. Dabei spielen insbesondere in der Photovoltaik nicht nur Großanlagen eine wichtige Rolle bei der Energieversorgung und Stabilisierung des Stromnetzes. Kleinere, privat oder auf gepachteten Dächern installierte Anlagen werden von Aggregatoren mit Hilfe von Energiespeichern längst zu größeren virtuellen Kraftwerken zusammengeführt.

Dadurch und im Zuge der Digitalisierung der Energiewirtschaft werden verteilte Erneuerbare Energieanlagen (EEA) zu stark vernetzten Infrastrukturen mit einem hohen Grad an Automatisierung und Fernsteuerung. Das wiederum erhöht das Risiko einer Störung der deutschen Energieversorgung durch Cyberangriffe. Schließlich bildet jede einzelne EEA eine Angriffsfläche. Und zentralisierte Leitstellen können zum Sprungbrett für Angreifende werden, um Tausende von Anlagen zu infiltrieren. Dabei besteht nicht nur das Risiko von Datenlecks und der Manipulation von Verbrauchsdaten. Es drohen lokale bis regionale Blackouts mit Verlusten und Strafen in Millionenhöhe. Im schlimmsten Fall können Anlagen irreparabel beschädigt und Menschenleben gefährdet werden.

Aus diesem Grund gelten für Akteure der deutschen Energieversorgung besondere gesetzliche Anforderungen an die Cybersicherheit. Mit dem NIS2-Umsetzungsgesetz (NIS2UmsuCG) werden die Anforderungen des bestehenden IT-Sicherheitsgesetzes (IT-SiG 2.0) maßgeblich erweitert und die Geschäftsführung persönlich haftbar gemacht.

Demnach gelten alle gewerblichen Energieerzeuger, Aggregatoren, Energiespeicherbetreiber und Stromlieferanten mindestens als »wichtige Einrichtungen«[1]. Viele fallen unter die Definition einer kritischen Anlage[2], für die ein System zur Angriffserkennung bereits seit IT-SiG 2.0 Pflicht ist. Auch wenn diese spezifische Maßnahme – wie andere Einzelmaßnahmen auch – nicht für wichtige Einrichtungen explizit genannt wird, laufen die Anforderungen aus dem NIS2UmsuCG auch für wichtige Einrichtungen auf dasselbe hinaus. Denn nur in der Kombination geeigneter organisatorischer und technischer Maßnahmen können die geforderten hinreichenden Sicherheitslevel erreicht werden.

Dieses eBook skizziert die unterschiedlichen Herausforderungen von Investoren, Geschäftsführungen und Betreibenden in Bezug auf EEAs. Das Dokument gibt einen detaillierten Überblick zu den real existierenden Cyberrisiken und formuliert darauf aufbauend klare Empfehlungen zur Gewährleistung einer nachhaltigen, effizienten Cybersicherheit in erneuerbaren Energieanlagen.

**Terminologische Konventionen**

Für kritische Infrastrukturen wird der mit NIS2 eingeführte Begriff der kritischen Anlagen verwendet.
Für die industrielle IT (Steuerungstechnik, Leit- und Fernwirktechnik, Prozessleittechnik) wird der etablierte Begriff der Operational Technology (OT) verwendet.
Erneuerbare Energieanlagen werden mit EEA abgekürzt.

**Disclaimer**

Dieses eBook entspricht keiner Rechtsbelehrung in Bezug auf geltende Cybersicherheitsgesetze und -verordnungen.

1 NIS2UmsuCG, Anlage 1, Juli 2024
2 KRITIS-Verordnung, Anhang 1 Teil 3, November 2023

## Inhalte des Whitepapers

# **OT-Sicherheit** ist für alle Stakeholder wichtig

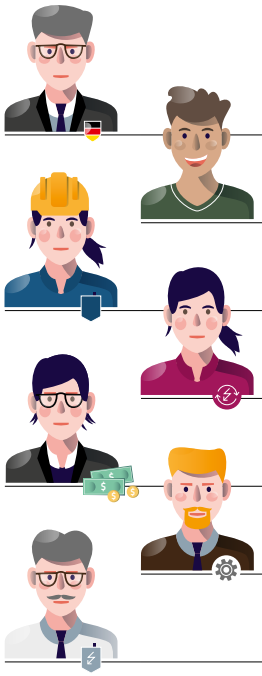
Die Energieversorgung ist wie kein anderer Sektor durch eine Vielzahl von Stakeholdern geprägt, die sich quer durch die Gesellschaft ziehen. Energieversorgungssysteme sind die Lebensadern unseres modernen Lebens. Verkürzt gesagt, leben allein in Deutschland rund 84 Millionen private und gewerbliche Stakeholder. Hinzu kommen die staatlichen Institutionen sowie die Investoren und Betreiber von EEAs. Für alle Stakeholder stellt die OT-Cybersicherheit eine Investition in den bestmöglichen Return on Investment (ROI) dar (Tabelle 1).

Trotz steigender Vorfälle, bei denen kritische Anlagen angegriffen wurden, wird die Investition in Cybersicherheit häufig kritisch betrachtet.[3] Cybersicherheit schafft keinen Wert, sondern erhält Wert. Der Return on Investment ist deshalb nicht direkt messbar. Der adäquate Indikator für die Effektivität von Cybersicherheitsmaßnahmen ist der Wert des verhinderten Verlustes. Dieser ist jedoch ebenso schwer zu berechnen, da der Verlust erst genau beziffert werden kann, wenn er eingetreten ist. Hilfreich sind deshalb Vergleichswerte.

So fand eine breit angelegte Studie heraus, dass Unternehmen mit einem soliden, ganzheitlichen Cybersicherheitsansatz die Kosten und Verluste durch Cybervorfälle jährlich um 26 % senken konnten.[4] In einer vorherigen Studie berichteten Unternehmen mit einer starken Cybersicherheit, dass sie 83 % aller Sicherheitsvorfälle detektieren konnten und in knapp der Hälfte der Vorfälle die Auswirkungen auf unter 24 Stunden begrenzen konnten. Im Vergleich dazu konnten Unternehmen mit weniger guter Sicherheits-Positionierung nur 54 % erkennen und hatten in 97 % aller Fälle länger als 24 Stunden mit den Vorfällen zu kämpfen.[5]

Der teilweise negativ wahrgenommene Einfluss von Cybersicherheitsinvestitionen auf den ROI von EEAs ist somit eine zu kurz gegriffene Rechnung, wenn nur die Ausgaben für die Maßnahmen betrachtet werden. Als Teil des Risikomanagement sollten die möglichen Verluste berücksichtigt werden, die in Schadensfällen auftreten würden. Vergleichswerte gibt es mittlerweile ausreichend aus gut dokumentierten Vorfällen, wie der WannaCry-Ransomware, dem Supply Chain Compromise bei SolarWinds oder dem Angriff auf den ukrainischen Energieversorger Ukrenergo in den Jahren 20215 und 2016. Die betroffenen Unternehmen standen in allen Fällen Zusatzkosten in mehrstelliger Millionenhöhe gegenüber.[6, 7] Hinzu kommen mögliche Strafzahlung für Nicht-Compliance in Bezug auf Cybersicherheitsgesetze.

Die Cybersicherheit Erneuerbarer Energieanlagen – und somit insbesondere die Sicherheit der industriellen Kommunikationsinfrastruktur (OT) – ist somit entscheidend beim Schutz des Return on Investment, der Anlagenverfügbarkeit und Netzstabilität.



| STAKEHOLDER | ZIELSETZUNG | RELEVANZ DER OT-SICHERHEIT |
|---|---|---|
| **Staat** | innere Sicherheit, soziale Ruhe und Stabilität | Abwehr feindlicher staatlicher Akteure, Vermeidung großflächiger Blackouts |
| **Private Endnutzer:innen** | Peace of Mind | Störungsfreier Alltag und Sicherheitsgefühl |
| **Gewerbliche Endnutzer:innen** | Geschäftsfähigkeit | Versorgungssicherheit der eigenen unternehmerischen Tätigkeit |
| **Private und gewerbliche Prosumer:innen** | Rentabilität eigener EEAs | Verfügbarkeit der eigenen EEAs |
| **Investor:innen** | Schneller, positiver ROI | Schutzes der Investition vor Ausfall, Beschädigung und Bußgeldern |
| **Anlagenbetreiber:innen, Aggregatoren** | Vermeidung von Zusatzkosten | Verfügbarkeit der EEAs, Integrität der Anlagendaten, Absicherung vor finanziellen und Haftstrafen |
| **Netzbetreiber** | Netzstabilität, Versorgungssicherheit | Vermeidung großflächiger Blackouts |

**Tabelle 1** OT-Sicherheit schützt die Interessen aller Stakeholder

3 Accenture »Building Greater Cyber Resilience in Renewables«, 2020
4 Accenture »State of Cybersecurity Resilience 2023«, 2023
5 Third Annual State of Cyber Resilience, 2020
6 *https://www.cybertalk.org/5-years-after-the-first-wannacry-attack* aufgerufen 17.09.2024
7 *https://heimdalsecurity.com/blog/solarwinds-attack-cost-impacted-companies-an-average-of-12-million* aufgerufen 17.09.2924

# **Risikolandschaft** von EEAs

Die Risikolandschaft von EEAs ist so vielfältig wie ihre Stakeholdergruppen. Sie reicht von geografischen über technologische bis zu geopolitischen Aspekten. Einige der Risiken lassen sich nicht auflösen. Sie bleiben als Restrisiko bestehen und können nur unter Kontrolle gebracht werden, indem sie überwacht werden.

## Geographisches Risiko

EEAs, insbesondere in großem Maßstab, werden an Standorten betrieben, die mitunter weit entfernt von jeglicher Zivilisation liegen. Doch selbst Privatanlagen in Wohnsiedlungen, die als virtuelles Kraftwerk geführt werden, sind aufgrund von Eigentumsgrenzen für Betreibende nicht zu jeder Zeit erreichbar. Eine wasserdichte physische oder personelle Absicherung der EEAs ist dadurch unmöglich. Angreifende haben alle Zeit der Welt, um eine EEA auszukundschaften, in diese einzubrechen und Anlagen zu manipulieren oder zu beschädigen. Schließlich befindet sich ein Großteil des digitalen Steuerungsequipments an oder in den EEAs. Einbrecher in einem Windrad haben Zugriff auf die lokalen speicherprogrammierbaren Steuerungen (SPS) und programmierbaren Automationssteuerungen (PAC) für die Energieproduktion, meteorologische Datenerfassung und Maschinensteuerung.[8] An Photovoltaik-Parks kann auf die Wechselrichter, lokale Steuerungseinheiten und Netzwerkkabel zugegriffen werden.

**So fern und doch so nah** Offshore-Windkraft ist schwer zu erreichen, aber nicht unerreichbar.

## Architektonisches Risiko

**Komplexität und Vereinfachung**

EEAs werden häufig mit bestehenden zentralen Energieanlagen und älteren IT/OT-System kombiniert, die meist keine oder nur geringe Cybersicherheitsmaßnahmen ermöglichen. Diese historisch bedingte Systemkomplexität braucht theoretisch eine strikte Segmentierung, um die unsicheren Systeme bestmöglich zu isolieren. Häufig wird die lokale OT in EEAs jedoch verhältnismäßig flach gestaltet, um die Komplexität zu reduzieren und eine stabilere Kommunikationsinfrastruktur zu ermöglichen.[9] Die flache Hierarchie führt zu einer geringen Segmentierung und erhöht somit das Risiko, dass Angreifende sich leichter durch das Netzwerk bewegen können (lateral und vertical movement).

**Örtliche Gegebenheiten**

Bei Freilandanlagen spielen auch die individuellen Gegebenheiten eine Rolle dabei, wie sicher die Anlage vor Fremdzugriff ist. Nicht immer ist es möglich, die Steuerungstechnik einer Anlage in einer verschlossenen Station unterzubringen. Bei Photovoltaikanlagen kommt es durchaus vor, dass Netzwerkleitungen frei ins Feld verlegt werden, wo Angreifende über Netzwerk-Taps unbemerkt Zugriff erlangen können.[10]

8 Utility Variable-Generation Integration Group, Wind Operating Practices Guidebook, Kap. 2.6.2, 2.6.3.
9 David Ferlemann, »Wind Farm Security Analysis and Attack Mitigation,« (Ph.D. Dissertation., University of Tulsa, 2017), 1–56.
10 BayWa r.e., H. Timm Elektronik, »Cyber Security in der Windindustrie«, 2021

**Internetverbindungen**

Weiterhin wird die Schnittstelle zwischen EEA und der zentralen Leitwarte der Betreibenden zu einem Risiko, wenn die Kommunikation nicht über eine dedizierte Kabelverbindung und stattdessen über das Internet erfolgt. Noch immer finden sich über die Internetplattformen Shodan und Censys Millionen industrieller Edge Devices in entlegenen Standorten, die über das Internet erreichbar sind. Nicht zuletzt private Anlagen auf Eigenheimen bieten eine Schnittstelle, über die nicht nur die Besitzerinnen und Besitzer, sondern auch Angreifende auf die Anlagensteuerung zugreifen können. Angreifende können so mitunter ortsunabhängig in die Anlagen eindringen.

**Das Fraunhofer Institut stellte dazu 2021 fest:** *»Diese technologische Komplexität, die internetbasierte Konnektivität und die heterogene Infrastrukturlandschaft schaffen einerseits Schwachstellen für Fehlfunktionen sowie Fehlbedienungen durch Mitarbeitende, wodurch die möglichen Angriffsflächen für Hacker vergrößert werden, und erschweren andererseits die Umsetzung von Sicherheitsstandards wie ISO/IEC 27001 und IEC 62443.«* [11]

**Die OT von Freilandanlagen** ist immer exponiert.

## Technologisches Risiko

**Unsichere Geräte**

Noch immer ist ein Großteil der aktuell erhältlichen und verbauten OT-Komponenten wie Switches, SPS, Wechselrichter etc. »insecure by design«. Der Grund ist einfach: Im Vordergrund der industriellen Digitalisierung stand und steht die Erhöhung der Verfügbarkeit und Prozessstabilität. Zugänge auf Systeme und Kommunikation zwischen Systemen sind deshalb häufig von Offenheit geprägt. Das zeigen auch immer wieder die Ergebnisse der Rhebo Industrial Security Assessments, bei denen eine detaillierte Schwachstellenanalyse der OT-Infrastruktur durchgeführt wird. Im Durchschnitt identifizieren die Rhebo OT-Expert:innen in jedem OT-Netzwerk 19 Sicherheitsrisiken und 7 Verfügbarkeitsrisiken (Abbildung 1, Seite 6).[12]

11 Fraunhofer Academy, »Aktuelle Herausforderungen für die Cybersicherheit in der Energieversorgung«, 2021

12 Rhebo, »OT-Risiken – Erkenntnisse aus Schwachstellenbewertungen 2023«, (letzter Zugriff, 02.10.2024)

## **TOP 10 SICHERHEITSRISIKEN** IN OT-NETZWERKEN 2023

Ergebnisse aus Rhebo Industrial Security Assessments in 2023

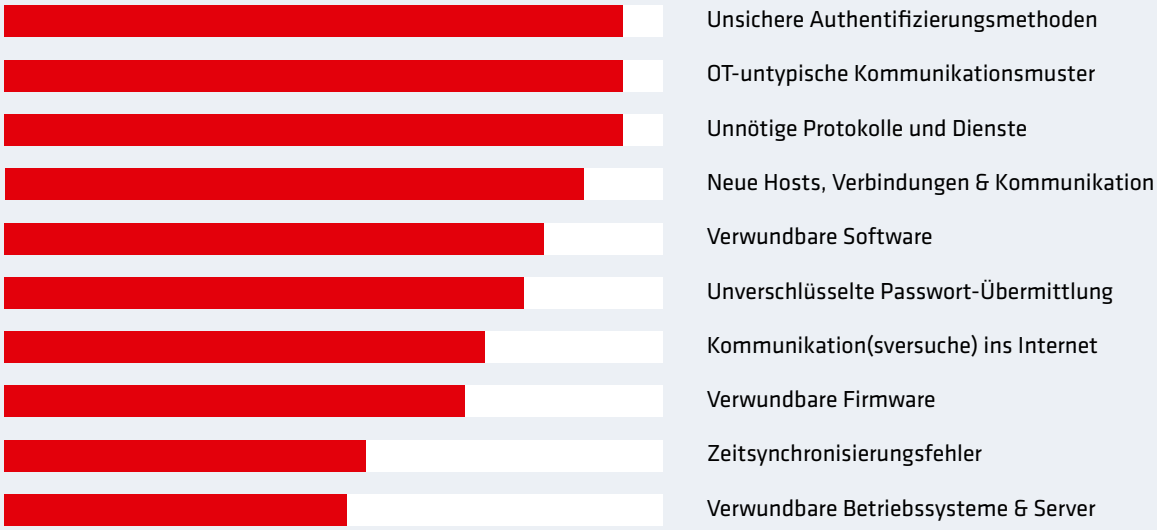
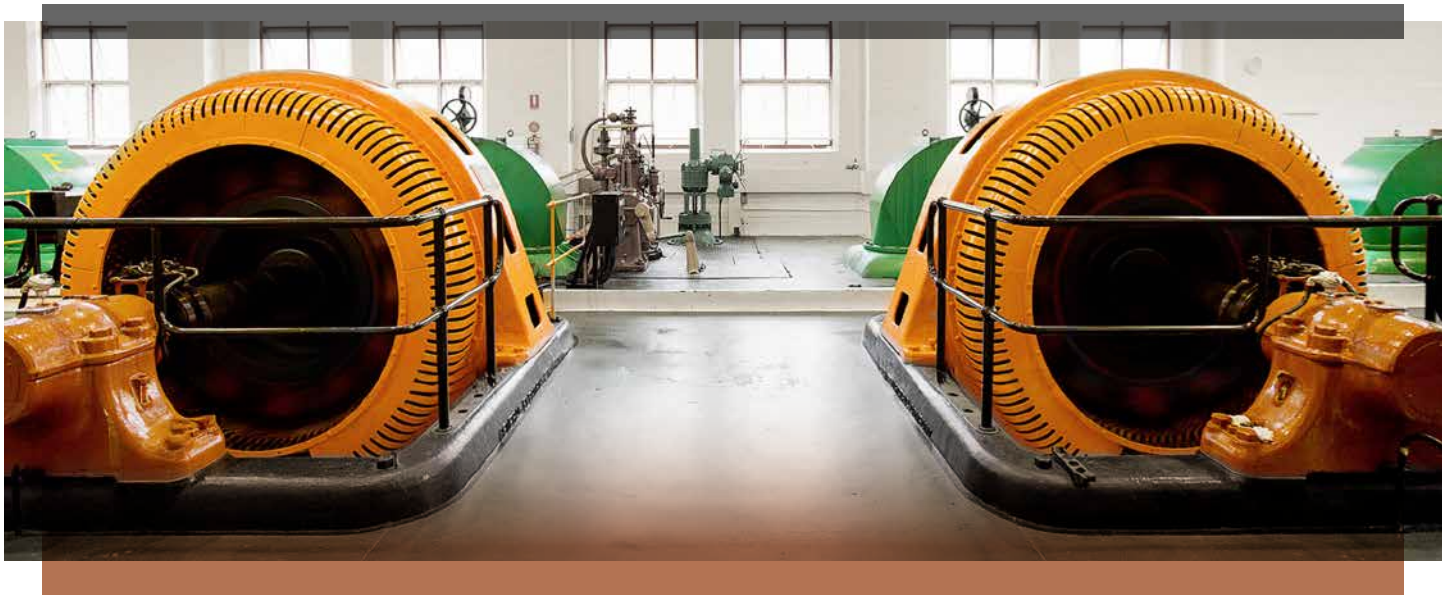



**Abbildung 1** In OT-Netzen finden sich versteckte Sicherheitslücken auf allen Ebenen, wie die Ergebnisse der Rhebo Industrial Security Assessments 2023 bei Kunden zeigen.

### Unsichere Protokolle

Ein Großteil der industriellen Kommunikationsprotokolle nutzen weder eine Authentifizierung, noch Verschlüsselungstechnologie. Selbst in modernen Anlagen, die dem IEC 61850 oder dem IEEE 1547-2018 Standard folgen, bleiben diese Sicherheitslücken bestehen. Beide Standards lassen die Protokollsicherheit komplett außen vor. Der 2023 veröffentlichte internationale Standard IEEE 1547.3 »IEEE Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems« argumentiert sogar, dass diese Standards die Cyberrisiken erhöhen ↗ siehe Kapitel 3. Zwar definieren Industriestandards wie IEC 62351-4 und IEC 62351-6 Sicherheitsmechanismen für die Protokolle MMS, GOOSE und SV. In der Praxis werden die zusätzlichen Absicherungen jedoch in der Regel nicht umgesetzt, weil sie ein erhöhtes Maß an Administration sowie eine höhere Run-Time-Memory benötigen. Letzteres kollidiert mit den Anforderungen an Echtzeitkommunikation in Energieinfrastrukturen.[13] Die inhärente Unsicherheit von OT-Komponenten und -Protokollen kann zwar erst wirklich ausgenutzt werden, wenn die Angreifenden im Netzwerk sind. Sie erleichtern ab diesem Punkt jedoch enorm die horizontale und vertikale Ausbreitung im Netzwerk sowie die Ausnutzung der einzelnen Systeme.



**Unsichere Protokolle** stellen auch in Wasserkraftwerken ein Risiko dar.

13 Rhebo, »360° Cybersicherheit in IEC 61850 Infrastrukturen«, 2023

### Unsichere Sicherheitssysteme

Selbst Geräte zur Sicherung der Netzwerkgrenze einer EEA können zum Unsicherheitsfaktor werden: Firewalls. Das prominenteste Beispiel stammt aus Dänemark. Im Mai 2023 wurde eine Zero-Day-Schwachstelle auf einer Firewall der Firma Zyxel bekannt. Binnen weniger Tage wurden 23 dänische Energieversorgungsunternehmen (EVU) Opfer von orchestrierten Angriffen, die diese Schwachstelle gezielt ausnutzten. Einige EVU mussten ihre OT isolieren und in den manuellen Betrieb der Anlagen umstellen.[14]

### KI-Systeme

Anwendungen mit künstlicher Intelligenz (KI) nehmen auch in der Energiewirtschaft zu. Bereits über 220 Unternehmen mit KI-Produkten sind im Energiesektor aktiv.[15] 74 % der Energieunternehmen gaben bei einer weltweiten Umfrage an, KI bereits einzusetzen oder es zu planen.[16] Aufgrund der Abhängigkeit der KI-Modelle von einem kontinuierlichen Datenstrom können KI-Systeme sowohl für Datendiebstahl, als auch für Datenmanipulation ausgenutzt werden. Letzteres kann dazu führen, dass ein KI-gesteuertes System fehlerhafte Entscheidungen trifft, die sowohl die EEA als auch die Netzstabilität beeinträchtigen.[17]

## Supply-Chain-Risiko

Die Lieferkette ist in allen Sektoren das schwächste Glied in der Cybersicherheit eines Unternehmens. Wenige Unternehmen haben einen ernsthaften Einfluss auf die Cybersicherheit ihrer Zulieferunternehmen. Wie der Fall SolarWinds 2020 zeigt, kann das verheerende Auswirkungen haben. Bereits im März 2020 wurde das Netzwerk des IT-Dienstleisters kompromittiert. Ziel war SolarWinds Kernprodukt, die Netzwerkmanagementplattform Orion. Die Plattform wurde zum damaligen Zeitpunkt von rund 15.000 Unternehmen genutzt. Die Angreifenden schafften es, Schadsoftware in ein Update einzuschleusen. Über dieses Update erhielten die Angreifenden Zugriff auf alle Kunden von SolarWinds, u.a. Regierungsbehörden, einige US-amerikanische IT-Sicherheitsunternehmen und Microsoft.[18] Solch ein Supply Chain Compromise kann jedoch auch ganz einfach über einen Wartungslaptop oder einen USB-Stick erfolgen, der durch externes Servicepersonal, z. B. bei Instandhaltungs- oder Wartungsarbeiten, an eine Anlage angeschlossen wird. Bereits der allererste bekannte Fall einer OT-Malware, Stuxnet im Jahr 2010, erfolgte über diesen Weg. Darüber hinaus ist die Zahl der Cybersicherheitsexpert:innen speziell für EEAs nach wie vor überschaubar. Der Fachkräftemangel auf diesem Gebiet – bei den EEA-Betreibern, Netzbetreibern und den Herstellern – stellt die größte Herausforderung bei der Umsetzung von OT-Sicherheit in EEAs dar.[19]

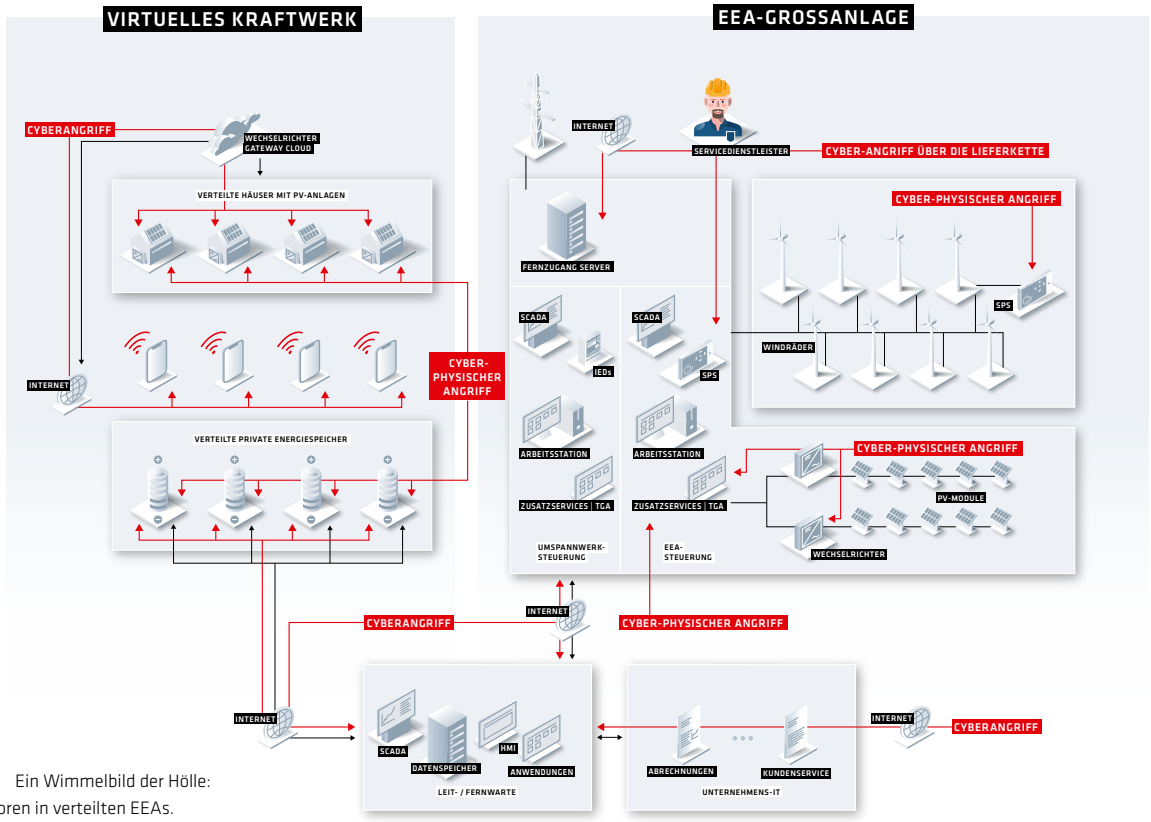



**Abbildung 2** Ein Wimmelbild der Hölle: Angriffsvektoren in verteilten EEAs.

14 SektorCERT, »Report: The attack against Danish, critical infrastructure«, November 2023
15 Vladimir Frank et al., »A Comprehensive Review of Artificial Intelligence (AI) Companies in the Power Sector«, Energies 2023, 16(3), 1077
16 IBM, »New IBM Study Data Reveals 74% of Energy & Utility Companies Surveyed Embracing AI«, 2024
17 Emily Newton, »The Dual Impact of AI on Power Grids: Efficiency and Vulnerability«, Revolutionized Magazin, 2024
18 Heise, »Cyber-Attacke über SolarWinds«, (letzter Zugriff: 02.10.2024)
19 IEEE, »IEEE 1547.3 - IEEE Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems«, 2023

**Die meisten sehen einen Installateur,** andere einen möglichen Supply Chain Compromise oder einen Hacker in guter Verkleidung.

### Stakeholder-Risiko

Wie schon in Kapitel 1 verdeutlicht, besitzen EEAs eine Vielzahl unterschiedlicher Stakeholder. Teilweise haben diese auch Zugang zu den Anlagen. Stakeholder haben direkt und indirekt Einfluss auf die Cybersicherheit ihrer EEAs. Das indirekte Risiko ergibt sich aus der Entscheidung, weniger in Cybersicherheit zu investieren, weil damit (vermeintlich) der ROI und der Unternehmensgewinn geschmälert würde. Das direkte Risiko ergibt sich aus einer gewissen Bequemlichkeit (im Englischen spricht man auch von Convenience). Weil der alltägliche Betrieb von EEAs sich umso einfacher gestaltet, je weniger Einschränkungen vorhanden sind, werden etablierte Sicherheitsmechanismen und Cyberhygiene-Regeln mitunter ausgehebelt oder missachtet. Wie in jeder Arbeitsumgebung schleifen sich informelle Workarounds ein, oder es wird auf Vertrauensbasis (vor allem gegenüber Dienstleistungsunternehmen) agiert.

### Geopolitisches Risiko

Nicht zuletzt wird die geopolitische Lage immer stärker zu einem Risiko für EEAs. Die Energiewende hat Erneuerbare Energien in Deutschland zum wichtigsten Energielieferanten gemacht. Entsprechend werden EEAs zu potenziellen Zielen für hybride Kriegsführung. Erst im Februar 2024 warnte die US-Amerikanische Cybersecurity & Infrastructure Security Agency (CISA) vor Aktivitäten der chinesischen Advanced Persistent Threat (APT) Volt Typhoon, die seit einiger Zeit Netzwerke kritischer Infrastrukturen infiltriert und sich in diesen strategisch platziert.[20] Dieses sogenannte Präpositionierung (Prepositioning) folgt einer langfristige Zielsetzung, die weniger auf eine kurzfristige Störung oder Ransomgeld-Forderung aus ist. Vielmehr geht es darum, im Rahmen der hybriden Kriegsführung bei einem künftigen Konflikt sofort handlungsfähig zu sein, sprich: die Infrastruktur gezielt zu stören. In diesem Sinne platziert Volt Typhoon an neuralgischen Punkten der gegnerischen Infrastruktur Schläferzellen, die nur noch auf den Aufwachbefehl warten.

## **Angriffsvektoren** in EEAs

EEAs bieten Angreifenden eine Vielzahl von Möglichkeiten, lokale Störungen der Energieversorgung zu provozieren, wie eine Studie des National Renewable Energy Laboratory und der Underwriters Laboratories 2021 hervorhebt.[21] Demnach können Angreifende:

- die Frequenz der netzaktiven Wechselrichter verändern,
- die Einstellungen für die Auslösespannung verändern,
- den Unterfrequenz-Lastabwurf (underfrequency load-shedding) deaktivieren,
- die Wechselrichtersteuerung übernehmen[22],
- die Anlagensteuerung übernehmen und
- Monitoringdaten manipulieren.

Typische Angriffe auf EEAs umfassen u.a.[23]:

- Eavesdropping: Ausspionieren und abgreifen von Kommunikation
- Masquerading: Zugriff über legitime Benutzerkonten per Stolen Credentials
- Man-in-the-middle: Einbringen eines zusätzlichen Gateways, über das in beide Richtungen (Aktuator, Kontroll-Center) manipulierte Kommunikation versendet wird
- Ressourcenerschöpfung or Denial-of-Service
- Replay: Kopieren eines Kommandos und Wiederverwendung zu einem späteren Zeitpunkt, um Störungen hervorzurufen
- Trojanisches Pferd (bzw. Angriff über Lieferkette)
- Wireless: Umschiffen der physischen Sicherheitssysteme über Wifi-fähige Komponenten

21 NREL, »Cybersecurity Certification Recommendations for Interconnected Grid Edge Devices and Inverter Based Resources«, 2021

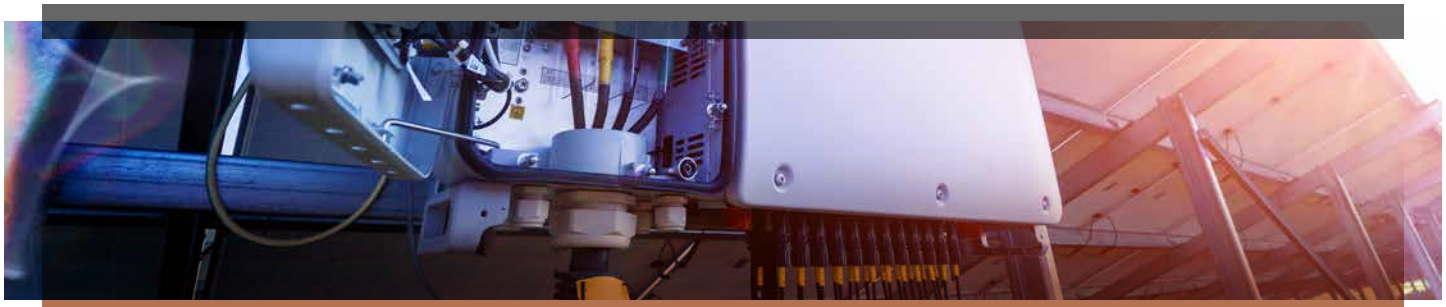
22 Johnson, Jay, Jimmy Quiroz, Ricky Concepcion, Felipe Wilches-Bernal, and Mathew J. Reno. 2019. »Power System Effects and Mitigation Recommendations for DER Cyberattacks.« IET Cyber-Physical Systems: Theory & Applications. https://doi.org/10.1049/iet-cps.2018.5014.

23 IEEE, »IEEE 1547.3 - IEEE Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems«, 2023, S. 35

## Angriffsvektoren und Störungen in Photovoltaik-Anlagen

In PV-Anlagen stehen vor allem die Wechselrichter sowie die Monitoring- und Steuerungssysteme im Fokus. Wechselrichter werden häufig mit Standardpasswörtern betrieben, besitzen selten eine physische Manipulationserkennung und verwenden aufgrund der langen Lebenszyklen mitunter angreifbare Chips.[24] Proof-of-Concepts haben bereits in der Vergangenheit gezeigt, dass über Fremdzugriff Referenzwerte so verändert werden können, dass ein Wechselrichter Blindleistung absorbiert und so zu einem Energieverlust führt. Weiterhin ist das Überladen von Batterien möglich.[25] Von Monitoring- und Steuerungssystemen können u.a. die Sensordaten manipuliert werden, um die Spannung zu verändern.[26] Weiterhin bildet die Verbindung zum Internet für die Datenübertragung im Zusammenhang mit einem schwachen Patchmanagement ein großes Einfallstor.

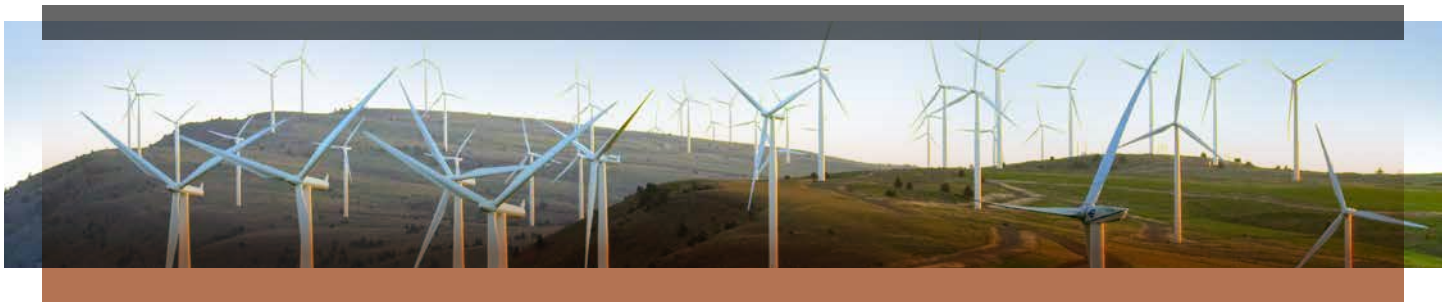
Die Zielsetzungen der Angreifenden werden mit der Größe der Nennleistung variieren. Präpositionierung und direkte Störungen der Netzstabilität und -versorgung werden nur in Großanlagen und größeren Verbünden einen Effekt erzielen. Kleinstanlagen werden selbst bei aggregierten virtuellen Kraftwerken weniger staatliche Angreifende interessieren. Kriminelle könnten in den tausenden von Gateways jedoch eine optimale Basis für ein Bot-Netzwerk, wie Mirai, finden. Jedoch ist die Größe der einzelnen Anlagen nicht zwangsläufig entscheidend, insbesondere wenn die Einspeisesteuerung über eine Drittanbieterplattform läuft, die Millionen solcher Kleinstanlagen koordiniert und damit Megawatt zu Gigawatt skaliert.[27]



**Die Steuerungstechnik in PV-Anlagen** ist digital und einfach erreichbar.

## Angriffsvektoren und Störungen in Windkraftanlagen

In vielen Windparks ist die OT dadurch geprägt, wenig segmentiert und stark vernetzt zu sein. Weitere Schwachstellen bilden die häufig schwache Autorisierung auf den Geräten[28] und eine fehlende Verschlüsselung der VPN-Verbindungen. Dienstleistungs- und Zulieferunternehmen haben nicht selten uneingeschränkten Zugriff per VPN, um die Anlagen zu monitoren, Systemsoftware zu aktualisieren und Wartungsarbeiten durchzuführen.[29] Das bietet Angreifenden eine große Angriffsfläche und vereinfacht die laterale Bewegung innerhalb der OT von Windparks. Der Zugang kann auch über die Glasfaserverbindungen und Ethernet Switches erfolgen. Aufgrund der entfernten Standorte von Windparks haben Angreifende eine gute Chance, Schaden anzurichten, bevor ein Einbruch bemerkt wird bzw. untersucht werden kann. Das Protokoll OPC XML-DA, das weit verbreitet zum Einsatz kommt, kann ausgenutzt werden, um falsche Daten zu Betriebszuständen zu versenden und den Betrieb bis zur Beschädigung der Anlage zu stören.[30]



**Windparks** sind generell für jeden Interessierten erreichbar.

24 Hill, Mark D., John Masters, Parthasarathy Ranganathan, Paul Turner, and John L. Hennessy. 2019. »On the Spectre and Meltdown Process Security Vulnerabilities.« IEEE Micro 39 (2): 9–19. *https://ieeexplore.ieee.org/abstract/document/8634886*

25 Bellini, Emiliano. 2020. »Solar Inverters vs. Cyber Attacks.« PV Magazine, August 17, 2020. *https://www.pv-magazine.com/2020/04/17/solar-inverters-vs-cyberattacks*

26 Watts, Raymond, Brian Kline, and Tom Ridge. 2018. Potential Electric Grid Vulnerability from Cyber Enabled Foreign Actors: A Risk Assessment Study of Solar Inverter Technology.

27 *https://www.bitdefender.com/en-us/blog/labs/60-hurts-per-second-how-we-got-access-to-enough-solar-power-to-run-the-united-states*

28 U.S. Department of Energy (DOE) Office of Energy Efficiency and Renewable Energy (EERE). 2020. Roadmap for Wind Cybersecurity. Washington, D.C.

29 Staggs, Jason, David Ferlemann, and Fugeet Shenoi. 2017. »Wind Farm Security: Attack Surface, Targets, Scenarios, and Mitigation.« International Journal of Critical Infrastructure Protection 17: 3–14

30 ebenda.

# **Rechtliche Anforderungen** an EEAs

Neben den ganz konkreten Risiken für die Cybersicherheit und den Betrieb von EEAs, stehen Anlagenbetreibende, -besitzer und -besitzerinnen heute einer weiteren Herausforderung gegenüber: Cybersicherheit rechtskonform in ihren Anlagen umzusetzen. Die derzeit wichtigsten rechtlichen Dokumente im deutschen Raum für EEAs sind:

- IT-Sicherheitsgesetz 2.0 mit Verweis auf das Energiewirtschaftsgesetz (EnWG)
- BSI-KRITIS-Verordnung
- EU NIS2 Direktive und das deutsche NIS2-Umsetzungsgesetz (NIS2UmsuCG)
- EU Cyber Resilience Act (CRA)

Die Gesetzgebung verweist dabei häufig auf den Stand der Technik. Tabelle 2 führt eine Auswahl nationaler und internationaler Cybersicherheit-Standards auf, die hierbei für EEAs Anwendung finden.

| | | |
|---|---|---|
| INTERNATIONALE STANDARDS | **ISO 27001** organisatorisch | Anforderungen an den Aufbau und Betrieb eines Managementsystem für Informationssicherheit (ISMS) |
| | **IEC 62443** organisatorisch, technisch | Basisstandard für Cybersicherheit in industriellen Infrastrukturen |
| | **IEC 62351** technisch | Sicherheit in Energiemanagementsystemen und zugehörigem Datenaustausch (Protokollsicherheit, Zugangskontrolle, Deep Packet Inspection, Sicherheitslogging) |
| | **IEEE 1547.3** technisch | Leitfaden für Cybersicherheit verteilter Energieressourcen und deren Anbindung an elektrische Energiesysteme → Aktuellster Standard für EEA-Cybersicherheit Ziel, die Resilienz der cyberphysischen Systeme zu stärken |
| | **NIST SP 1800-32** organisatorisch | US-amerikanischer Industriestandard für die Cybersicherheit verteilter Energieressourcen als Beispiel von IIoT-Sicherheit |
| | **NIST SP 800-82 Rev.3** organisatorisch | US-amerikanischer Industriestandard für Cybersicherheit in OT-Netzen |
| NATIONALE STANDARDS | **B3S Aggregatoren** | Branchenspezifischer Sicherheitsstandard für Anlagen oder Systeme zur Steuerung/Bündelung elektrischer Leistung |
| | **BDEW / OEE / VSE Whitepaper** | Anforderungen an sichere Steuerungs- und Telekommunikationssysteme von Energieversorgungsunternehmen entlang der gesamten Lieferkette |
| | **BSI Orientierungshilfe** zum »Einsatz von Systemen zur Angriffserkennung« | Handreichung, welche die grundlegenden Anforderungen an ein System zur Angriffserkennung im Sinne des IT-SiG 2.0 definiert. |
| | **ICS Security Compendium** | Grundlagenwerk des BSI zur OT-Sicherheit |
| | **CISIS12** | Compliance Informations-Sicherheitsmanagement System in 12 Schritten für Kommunen und KMUs |
| | **TRBS 1115 Teil 1** | Technische Regeln für die Cybersicherheit sicherheitsrelevanter Mess-, Steuer- und Regeleinrichtungen |
| | **VdS 10000** | Informationssicherheitsmanagementsystem für KMUs mit Fokus auf die IT |

**Tabelle 2** Auswahl der wichtigsten Standards für EEAs

## IT-Sicherheitsgesetz 2.0

Das im Mai 2021 aktualisierte IT-Sicherheitsgesetz (IT-SiG 2.0) ist ein Mantelgesetz, das Cybersicherheitsanforderungen in mehreren bestehenden Gesetzen ergänzt. Für EEAs sind die wichtigsten Gesetze:

- das BSI-Gesetz, §8a (1a),
- das Energiewirtschaftsgesetz (EnWG), §11 (1d).

In beiden Gesetzen werden Betreibende von Anlagen nach BSI-KRITIS-Verordnung und/oder Energieversorgungsnetzen verpflichtet, ein System zur Angriffserkennung (SzA) zu betreiben, das ihre OT absichert. Hierfür veröffentlichte das BSI 2022 eine Orientierungshilfe zum »Einsatz von Systemen zur Angriffserkennung«, in denen die geforderten Funktionalitäten definiert werden.[31]

## BSI KRITIS-V: Kritische Anlage? Ja oder Nein?

Die BSI-Verordnung definiert, welche Anlagen als kritische Infrastruktur (KRITIS) bzw. nach NIS2 als kritische Anlage eingestuft werden. Entsprechend der Anlage 1, Teil 3 der Verordnung gelten Energieerzeugungsanlagen als KRITIS:

1. in allen Fällen ab einer installierten Nettonennleistung von >104 MW.
2. bei Betrieb einer Schwarzstartanlage ab einer installierten Nettonennleistung von >0 MW. Ein Schwarzstart beschreibt die Wiederinbetriebnahme des Energienetzes nach einem flächendeckenden Stromausfall.
3. bei Betrieb einer Anlage zur Erbringung von Primärregelleistung ab einer installierten Nettonennleistung von >36 MW. Primärregelanlagen werden genutzt, um kurzfristig (binnen 30 Sekunden) Schwankungen im Stromnetz auszugleichen.

Erneuerbare Energieanlagen benötigen in der Regel Speichersysteme, um für die Erbringung von Primärregelleistung (Punkt 3) in Betracht zu kommen, da die Verfügbarkeit jederzeit sichergestellt sein muss. Ob die eigene EEA als kritische Anlage,Schwarzstart- oder Primärregelanlage gilt, sollte unbedingt mit einem Rechtsbeistand und den Netzbetreibern geklärt werden. Der Schwellenwert kann auch über virtuelle Kraftwerke erreicht werden, in denen eine Vielzahl von Kleinstanlagen zusammengefasst gesteuert werden. Das deutsche Unternehmen sonnen GmbH betreibt zum Beispiel seit 2018 ein virtuelles Kraftwerk, in dem über 25.000 private Haushalte mit ihren Sonnen Energiespeichern rund 250 MW an Kapazität aufbringen.[32] Sonnen betreibt deshalb bereits seit 2019 ein softwarebasiertes OT-Monitoring mit Angriffserkennung von Rhebo auf all ihren Energiespeichern.

**IIOT SECURITY**
Angriffserkennung auf Sonnen Energiespeichern

Referenzstory herunterladen

## NIS2 und das NIS2UmsuCG

Das deutsche NIS2UmsuCG erweitert die Anzahl der Unternehmen, für die Cybersicherheit gesetzliche Pflicht wird, von ein paar Tausend auf knapp 30.000. Für Akteure in der Energiewirtschaft verändert sich vor allem die Reichweite ihrer Verpflichtungen. Neben der kritischen Anlage und deren OT muss nun das gesamte Unternehmen cybersicher sein. Im Falle der Einordnung als kritische Anlage nach BSI-KRITIS-Verordnung gilt weiterhin, dass ein ganzheitliches Angriffserkennungssystem zu betreiben ist. Weiterhin fordert das NIS2UmsuCG ein Cyberrisikomanagement unter Einbeziehung der Lieferkette. Unter anderem müssen kritische Komponenten nachweislich sicher sein (Artikel 1 § 41 (3) NIS2UmsuCG). Als kritische Komponenten gelten IKT-Produkte, die in kritischen Anlagen verbaut werden oder deren Störung die Funktionsfähigkeit oder Sicherheit der kritischen Anlage erheblich beeinträchtigen. Die Geschäftsführung wird erstmals für die Nichteinhaltung der Sicherheitsanforderungen persönlich haftbar gemacht.


**NIS2-ANFORDERUNGEN IN DER OT**
Herausforderungen und Limitierungen

Whitepaper herunterladen

## Cyber Resilience Act

Der Cyber Resilience Act (CRA) der EU zielt vor allem auf alle herstellenden Unternehmen, die Komponenten mit digitalen Schnittstellen oder Anwendungen im europäischen Markt verkaufen wollen. Die Anforderungen an integrierte Cybersicherheit (»secure by design«) werden verpflichtender Bestandteil für den Erhalt des CE-Kennzeichens und somit Voraussetzung für den Zutritt auf den europäischen Markt. Um Unternehmen einen klaren Fahrplan zu geben, werden derzeit die verschiedenen existierenden Sicherheitsstandards harmonisiert. Sehr wahrscheinlich wird der Standard IEC 62443 und hier die Kapitel 4–1 »Secure product development lifecycle requirements« und 4–2 »Technical security requirements for IACS components« eine Rolle spielen, die explizit Cybersicherheitsvorgaben für OT-Komponenten definieren.

31 BSI, »Orientierungshilfe zum ›Einsatz von Systemen zur Angriffserkennung‹«, 2022
32 *https://www.mdr.de/wissen/sind-virtuelle-kraftwerke-die-zukunft-102.html* (letzter Zugriff 08.10.2024)

# **Angriffserkennung** in EEAs

Die Standards aus Kapitel 3 definieren eine Vielzahl an technischen Maßnahmen, lassen betroffene Unternehmen aber schnell den Blick fürs Ganze verlieren. Eine Ansammlung von Tools macht eine EEA noch nicht sicher. Sie müssen im Zusammenspiel dem Ziel dienen, die Cybersicherheit und Cyberresilienz der EEAs dauerhaft zu gewährleisten. Cybersicherheit sollte deshalb drei Prämissen folgen:

1. Defense-in-Depth,
2. Cyber Resilience Ende-zu-Ende,
3. Kontinuierlicher Verbesserungsprozess.

## Defense-in-Depth in EEAs

Es gibt keine 100%-ige Cybersicherheit. Cybersicherheit bleibt für Angreifende und Abwehrende ein ständiges Katz- und Mausspiel. Ein erfolgreicher Cyberangriff ist keine Frage des »ob«, sondern des »wann«. Diese Realität wird durch zwei Entwicklungen befeuert:

1. Durch die wachsende Vernetzung und Digitalisierung von Infrastrukturen, wird die digitale Domäne kurzfristig zu einem lukrativen kriminellen Geschäft und strategisch zu einem entscheidenden Schauplatz in staatlichen Konflikten.
2. Künstliche Intelligenz erlaubt die schnellere Weiterentwicklung von Angriffstechniken.

Wie schon in Kapitel 2 verdeutlicht, bleiben in jedem Fall auf verschiedenen Ebenen Restrisiken für die Cybersicherheit bestehen. Diese können zwar nicht direkt abgewehrt, aber unter Kontrolle gebracht werden. Die effektivste Option ist es, Cybersicherheit als mehrstufige Strategie von außen nach innen aufzubauen. Dieses aus dem Militär abgeleitete Konzept des Defense-in-Depth zielt darauf, bei erfolgreichen Angriffen, z. B. einem Fremdzugriff auf das OT-Netzwerk oder OT-Komponenten in EEAs, noch immer in der Lage zu sein, die Angreifenden aufzuhalten. Mit Firewalls und einem Security Information & Event Management System (SIEM) allein ist dies nicht möglich.

Das internationale Institute of Electrical and Electronics Engineers (IEEE) warnt entsprechend: *»Die Sicherheit des intelligenten Stromnetzes muss eine ›Defense-in-Depth‹-Strategie beinhalten, die mehrere Sicherheitsstufen umfasst, da jede Lücke dazu führen könnte, dass Angreifer oder sogar unbeabsichtigte Fehler und Ausfälle die Sicherheit der Menschen und die Zuverlässigkeit des Stromnetzes erheblich beeinträchtigen.«*[34] Ein modernes, stark interaktives Netzwerk muss – um es an einer Analogie zu erläutern – wie ein moderner Staat bzw. wie ein Stadtstaat gesichert werden (Abbildung. 3). Der Stadtwall, die Torwächter und das Militär (Firewalls, Datendioden, Authentifizierung, physische Zugangskontrollen) sichern den Staat nach außen. Die Bewohner:innen (Belegschaft, Dienstleister) haben die Gesetzgebung als Maßstab (ISMS, Compliance- und Sicherheitsleitlinien). Für die Innere Sicherheit im Land sind Polizei und Verfassungsschutzbehörden (Anomalieerkennung, netzwerkbasiertes und Edge Device basiertes Angriffserkennungssystem) zuständig. Die äußeren und inneren Gefahren werden schließlich von den Geheimdiensten zu einem Gesamtlagebild (SIEM) zusammengeführt. Angreifende, die es schaffen, sich in den Stadtstaat zu schleichen, können dadurch schneller entlarvt und gestellt werden. Außerdem wird ihnen die Ausbreitung im Inneren erschwert.

> *»Defense-in-Depth umfasst die Kombination mehrerer heterogener Sicherheitstechnologien für die gängigen Angriffsvektoren, um sicherzustellen, dass Angriffe, die von einer Technologie übersehen werden, von einer anderen erkannt werden«.*[33]

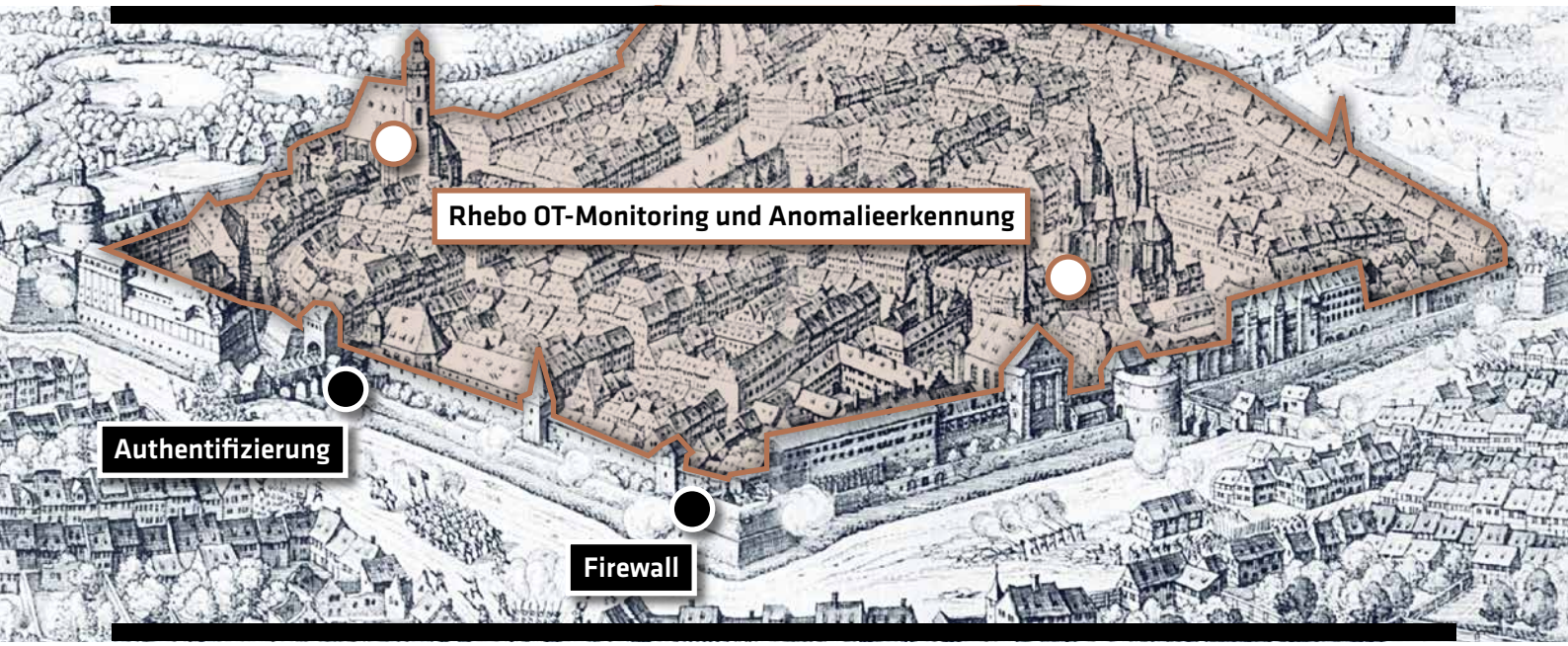



**Abbildung 3** Ein OT-Netzwerk muss wie eine Stadtfestung gesichert sein. Dazu gehört auch die Innere Sicherheit.

Viele Unternehmen verlassen sich noch immer auf den Stadtwall und die Gesetzgebung, in der Hoffnung, niemand Feindliches wird es je hinter die Tore schaffen. Wie fahrlässig dieser Ansatz ist, zeigt nicht nur der Fall des ukrainischen Energieversorgers Ukrenergo im Jahr 2016. Angreifende hatten sich im Januar 2016 per Spear Phishing Zugang in das Netzwerk des Unternehmens verschafft. Sie bewegten sich danach ganze zehn Monate unentdeckt durch die IT und weitere 17 Tage durch die OT, bevor sie am 17.12.2016 einen Blackout provozierten, der 20 % der Hauptstadt Kyjiw ohne Strom zurückließ. Noch aktueller ist die Analyse der US-amerikanischen CISA im Februar 2024, dass sich staatlich gestützte APTs teilweise seit Jahren fest in Netzwerken kritischer Anlagen bewegen, um für den Fall der Fälle einsatzbereit zu sein.

Sowohl der Vorfall als auch die neuesten Entwicklungen und das verbleibende Restrisiko sprechen eindeutig für die Notwendigkeit der Inneren Sicherheit in OT-Netzwerken. Das in Abbildung 4 versinnbildlichte Monitoring mit integrierter Anomalie- und Angriffserkennung untersucht die OT-Kommunikation auf Vorgänge, die vom bestehenden, etablierten Muster abweichen. Das ist in der OT möglich, da industrielle Anlagen durch sich wiederholende, vorhersehbare Kommunikation geprägt sind. Aktivitäten von Angreifenden sind deshalb relativ leicht von der legitimen Kommunikation unterscheidbar. Dadurch sieht das Angriffserkennungssystem auch Angreifende, die über neuartige Angriffstechniken, unbekannte Schwachstellen, gestohlene Zugangsdaten und Supply Chain Compromise in die OT gelangt sind, ohne die Firewalls und das SIEM-System in Alarm versetzt zu haben.

Das BSI sprach sich deshalb bereits 2021 in einem Arbeitspapier für den Einsatz eines Monitoring mit Anomalieerkennung in der OT-Cybersicherheit aus.[35] Diese Empfehlung wurde mit der Verankerung eines Systems zur Angriffserkennung im IT-SiG 2.0 und dem NIS2UmsuCG weiter gestärkt.

Das OT-Sicherheitsmonitoring bildet im Sinne des Defense-in-Depth-Ansatzes die »2nd line of defense«, um sowohl Innentäter:innen als auch erfolgreiche Angriffe in den Netzwerken frühzeitig zu erkennen, und dadurch die Reaktionsfähigkeit von Unternehmen zu stärken. Perimeter-Sicherung, übergreifendes SIEM-System und OT-Monitoring gehen in der Cybersicherheit von EEAs Hand in Hand (Abbildung 4).

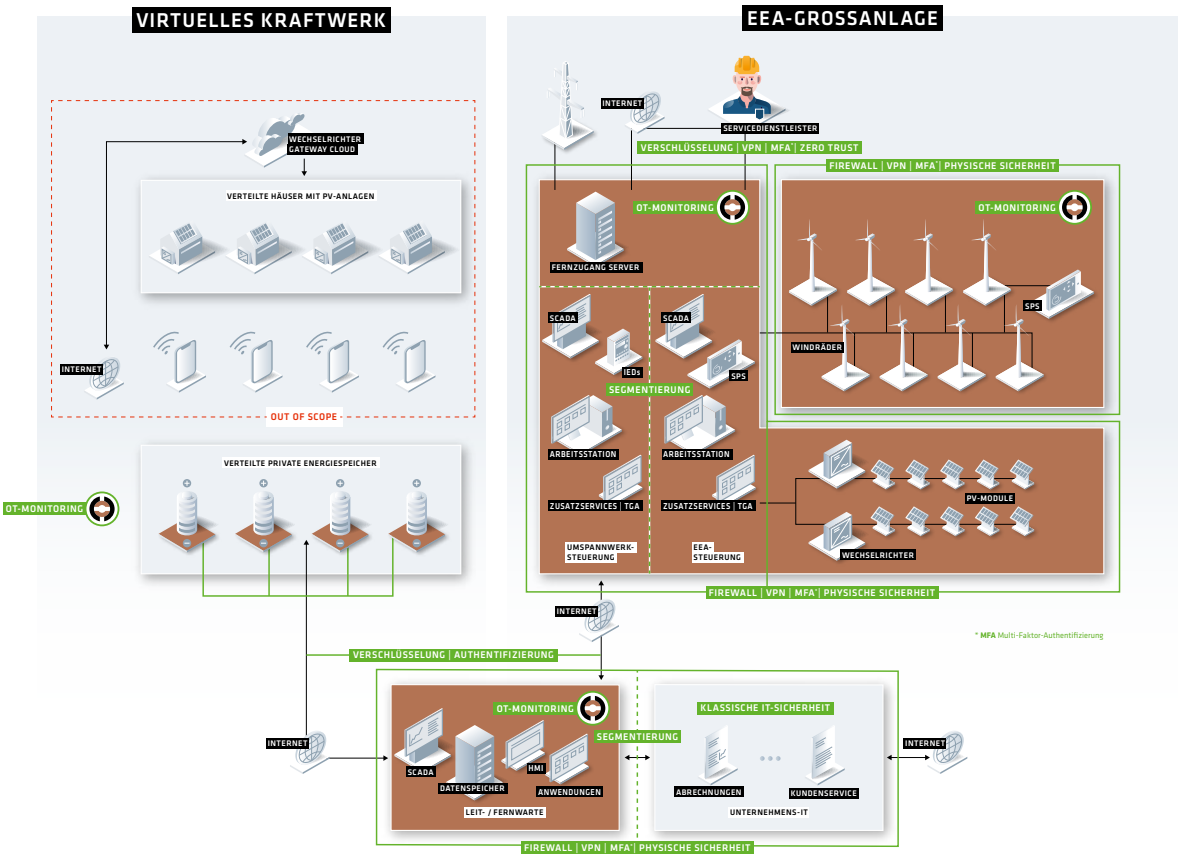



**Abbildung 4** Beispielhafte Defense-In-Depth-Architekturen in großen EEAs (rechts) und virtuellen Kraftwerken (links).
Zusätzlich sollten alle Komponenten (SPS, Wechselrichter, Energiespeicher, SCADA, IEDs etc.) secure by design entwickelt werden.

33 z. B. NIST SP 800-171, NIST SP 800-172, NISTIR 8183

34 IEEE, »IEEE 1547.3 – IEEE Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems«, 2023, S. 25

35 *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Vorfaelle/log4j-Schwachstelle-2021/log4j_Schwachstelle_Detektion_Reaktion.html* (letzter Zugriff 09.10.2024)

## Cyber Resilience in EEAs

Fast alle Standards und auch NIS2 folgen dem Prinzip der Eskalation eines Angriffs, die auch in Defense-in-Depth steckt. Cyberresilienz nimmt zusätzlich die Zeit nach einem abgewehrten Angriff hinzu, in der es darum geht, die Cybersicherheit zu stärken und die Systeme wiederherzustellen. Die Berücksichtigung aller Aspekte der Cyberresilienz ermöglicht Unternehmen, entlang der gesamten Entwicklung eines Cyberangriffs handlungsfähig zu bleiben:

## 1 PRÄVENTIONSMASSNAHMEN beim versuchten Angriff

### 1.1 Mitarbeiter schulen

- Best Practices der Cybersicherheit, Cyberhygiene und Passwortvergabe
- Sensibilisieren für Phishing-Angriffe und Social Engineering

### 1.2 OT-Schwachstellen schließen

- Risikoanalyse und Schwachstellenanalyse
- Assets (Geräte, Systeme, Verbindungen) identifizieren und dokumentieren
- Kritische Assets kategorisieren
- Patch-Management aufbauen inkl. Information durch CISA und BSI, Testumgebung, Roll-out-Plan

### 1.3 Zugang zum Netzwerk und zu Systemen erschweren

- Physische Absicherung
- Zugangsbeschränkungen
- Zugriffsbeschränkungen (Zero Trust)
- Autorisierung über Role-based Access Control (RBAC)
- Netzwerk-Segmentierung

### 1.4 Mobile Geräte absichern

- Freigabe-, Dokumentations- und Patchprozess für USB-Sticks, Laptops und mobile Endgeräte

### 1.5 Authentifizierungsmaßnahmen implementieren

- Multi-Faktor-Authentifizierung für Geräte und Systeme
- Starkes Passwortmanagement
- Shared Accounts verhindern

### 1.9 Sicherheitssystem regelmäßig überprüfen

- Regelmäßige Schwachstellenbewertung und Risikoanalyse
- ggf. Pentests
- Regelmäßige Prüfung der Einhaltung der Sicherheitsrichtlinien

### 1.8 Compliance sicherstellen

- Gesetze und Regularien bewerten
- Umsetzung dokumentieren
- Audits (intern / extern)

### 1.7 Lieferkette einbeziehen

- Lieferkettenrisiken (Schnittstellen, Zugriffe etc.)
- Lieferantenauswahl (Dual Sourcing)
- Cybersicherheitsrichtlinien und -audits für Dienstleister und Hersteller
- Multi-Faktor-Authentifizierung und Verifizierung durch Administrator:in
- Zero-Trust, klare Zugriffsbeschränkungen,
- Cybersicherheit als Vertragsbestandteil

### 1.6 OT-Kommunikation absichern

- Unsichere Protokolle entfernen oder überwachen
- Verschlüsselungsstandards für Protokolle z.B. IEC 62351-4, IEC 62351-9)
- Authentifizierungsstandards für Protokolle (z.B. IEC 62351-6)

## 2 DETEKTIONSMASSNAHMEN beim erfolgreichen Angriff

### 2.1 Fremdzugriffversuche erkennen

- Physische Überwachung (Kameras, Sensoren)
- Logging der Anmeldungen
- Limitierung der Anmeldeversuche
- Firewalls

### 2.2 Verdächtige Vorgänge / Kommunikation im Netzwerk erkennen

- OT Monitoring mit Anomalie- und Angriffserkennung
- SIEM (als Gesamtsystem für IT & OT)

## 3 REAKTIONSMASSNAHMEN für die Abwehr eines erfolgreichen Angriffs

### 3.1 Notfallkommunikation etablieren

- Verantwortlichkeiten
- Kommunikationshierarchie
- Gesetzliche Meldepflichten

### 3.2 Incident Response Plan etablieren

- Forensische Analyse
- Eingrenzung des Vorfalls und Isolierung der betroffenen Systeme und Netzwerke

### 3.3 Betrieb sicherstellen

- Redundante Systeme
- Kurzfristige Wiederherstellung kritischer Systeme

## 4 RECOVERYMASSNAHMEN nach der Abwehr eines Angriffs

### 4.1 Business Continuity Management etablieren

- Multiple, autarke Backups
- Prozess für Rückkehr zum Normalbetrieb

### 4.2 Cybersicherheit verbessern

- Forensische Analyse
- Neubewertung der Risikoanalyse
- Anpassung der Richtlinien, technischen und organisatorischen Maßnahmen

## Cybersicherheit hört nie auf

Cybersicherheit ist kein Endzustand, sondern ein ständiger Berg-auf-Kampf. Bereits vor mehreren Jahren berichtete das BSI von über 400.000 neuen Malware-Signaturen pro Tag. Durch KI, die Ausweitung hybrider Kriegsführung und die Zunahme cyberkrimineller Gruppierungen wird der Druck in der Cybersicherheit nur noch beschleunigt.

Die Cybersicherheit (Security Posture) und die Risikolage müssen deshalb auch in EEAs regelmäßig überprüft werden und dem aus dem Qualitätsmanagement bekannten Kontinuierlichen Verbesserungsprozess (Abbildung 5) folgen. Wichtige Schritte sind:

- Regelmäßig Informationen über neue bekannt gewordene und ausgenutzte Schwachstellen in OT-Komponenten einholen. Hierfür empfehlen sich die ICS Security Alerts der CISA, die täglich über neue Meldungen informieren und oftmals Handlungsempfehlungen aussprechen.[36]
- Wiederholte Schwachstellenanalysen untersuchen in regelmäßigen Zyklen die OT auf bestehende und neue Sicherheitslücken (z. B. mit dem Service Rhebo Industrial Security Assessment).
- Durch das OT-Monitoring identifizierte Anomalien analysieren. Bei Bedarf Unterstützung durch Expert:innen des Herstellers einholen, um das eigene Wissen zu OT-Risiken im Unternehmen aufzubauen (z. B. mit dem Service Rhebo Managed Protection).

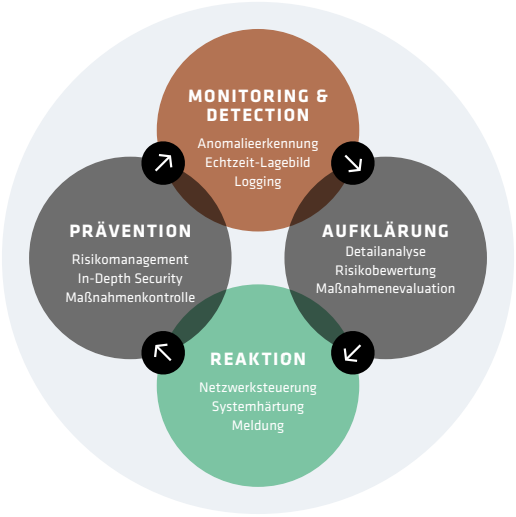
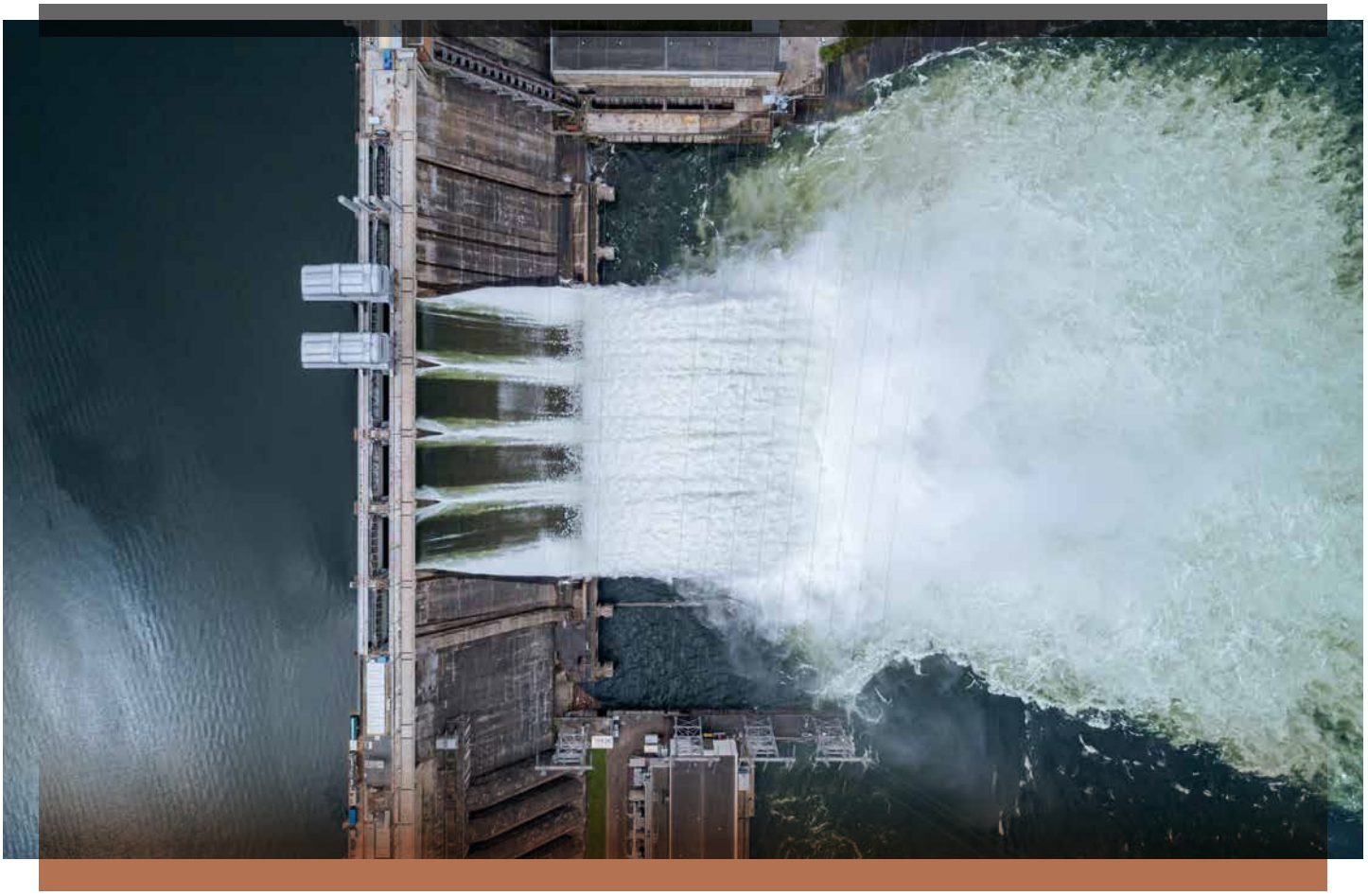



**Abbildung 5** Cyberresilienz und Cybersicherheit bleiben nur erfolgreich, wenn die Maßnahmen regelmäßig auf ihre Effektivität geprüft und aus Vorfällen gelernt wird.



36 *https://www.cisa.gov/resources-tools/resources*

# 3 Schritte zur Cybersicherheit von EEAs

## 1


Der erste einfache Schritt
zu umfassender OT-Sicherheit:
**Rhebo Industrial Security Assessment**

### Cybersicherheit beginnt mit Sichtbarkeit.

Die Rhebo OT-Risikoanalyse und Reifegradbeurteilung des **Rhebo Industrial Security Assessment** liefert ein detailliertes Verständnis der OT-Assets, der Netzwerk- und Kommunikationsstruktur sowie bestehender Sicherheitsrisiken. Unsere Kunden erhalten einen umfassende Übersicht und klare, effektive Handlungsempfehlungen, um die Systemhärtung zu steigern.

### Sie profitieren von

- der Identifikation aller Geräte und Systeme in der OT inklusive ihrer Eigenschaften, Firmware-Versionen, Protokolle und Kommunikationsverbindungen (Asset Discovery & Inventory);
- der detaillierten Analyse bestehender Schwachstellen nach CVE;
- der Identifikation bestehender Gefährdungen, Sicherheitslücken und technischer Fehlerzustände;
- Handlungsempfehlungen mit Abschlussbericht und Workshop.

## 2


Der nahtlose Übergang zu
durchgängiger OT-Sicherheit:
**Rhebo Industrial Protector**

### OT-Sicherheit endet nicht an den Netzwerkgrenzen.

Das OT-Monitoring mit integrierter Angriffserkennung **Rhebo Industrial Protector** schafft dedizierte OT-Sicherheit entsprechend der NIS2. Es erweitert die Absicherung durch Firewalls um eine ganzheitliche Anomalieerkennung innerhalb der OT, ohne kritische industrielle Prozesse zu stören. Die Lösung steht als Agent-Version auch für Edge Devices wie Energiespeicher zur Verfügung.

### Sie profitieren von

- der Echtzeit-Sichtbarkeit des Kommunikationsverhaltens aller OT- und ICS-Geräte (Protokolle, Verbindungen, Datenraten);
- der Echtzeitmeldung und -lokalisierung von Vorgängen (Anomalien), die auf Cyberattacken, Manipulation und technische Fehlerzustände hinweisen;
- der frühzeitige Identifikation von Angriffen über Backdoors, bislang unbekannte Schwachstellen und Innentätern, die von Firewalls übersehen werden (Defense-in-Depth)

## 3


Wir überwachen, damit Sie sich
um Ihr Kerngeschäft kümmern können:
**Rhebo Managed Protection**

### OT-Sicherheit braucht Ressourcen und Know-How.

Rhebo unterstützt Sie mit **Rhebo Managed Protection** beim Betrieb des OT-Sicherheitsmonitorings mit Anomalieerkennung, insbesondere bei der Auswertung und Reaktion auf Vorfälle sowie der kontinuierlichen Überprüfung und Verbesserung der Abwehrmechanismen.

### Sie profitieren von

- der Unterstützung unserer Expert:innen beim Betrieb des OT-Sicherheitsmonitorings;
- der schnellen forensischen Analyse und Aufklärung von OT-Anomalien;
- der schnellen Handlungsfähigkeit bei Vorfällen;
- regelmäßigen OT-Risikoanalysen für die kontinuierliche Verbesserung des Reifegrads Ihrer Cybersicherheit.

# Schützen Sie Ihre Erneuerbare Energieanlagen
## vor Cyberangriffen und Compliance-Strafen


**Rhebo OT Security**
Umfassende Cybersicherheit
für industrielle
Steuerungsnetze


**Rhebo Industrial**
**Security Assessment**
Risikobewertung
und Schwachstellenanalyse


**Rhebo IIoT Security**
Angriffserkennung
für Edge Devices
und IIoT Endpunkte

www.rhebo.com | sales@rhebo.com | +49 341 3937900

ISO/IEC 27001 | OT SECURITY Made in Germany | CYBERSECURITY MADE IN EUROPE™ Initiated by ECSO. Issued by eurobits e.V. | bitkom

**Rhebo** OT Security Made Simple

Rhebo bietet einfache und effektive Cybersicherheitslösungen für die Netzleit-, Fernwirk- und Steuerungstechnik sowie verteilte industrielle Anlagen in Energieunternehmen, Kritischen Infrastrukturen und Industrieunternehmen. Das deutsche Unternehmen unterstützt Kunden auf dem gesamten Weg der OT-Sicherheit von der initialen Risikoanalyse bis zum betreuten OT-Monitoring mit Anomalie- und Angriffserkennung. Rhebo ist seit 2021 Teil der Landis+Gyr AG, einem global führenden Anbieter integrierter Energiemanagement-Lösungen für die Energiewirtschaft mit weltweit rund 7.500 Mitarbeiter:innen in über 30 Ländern. Als vertrauenswürdiges Cybersicherheitsunternehmen ist Rhebo nach ISO 27001 zertifiziert sowie Partner der Allianz für Cyber-Sicherheit des Bundesamts für Sicherheit in der Informationstechnik (BSI) und offizieller Träger des Gütesiegels »Cybersecurity Made In Europe«.

*www.rhebo.com*

**Rhebo GmbH** Spinnereistraße 7 | 04179 Leipzig | Deutschland
**rhebo.com**

**EBOOK EEA | 11-2024** | © Rhebo GmbH
Alle Angaben ohne Gewähr. Änderungen vorbehalten.
Bildmaterial: Pixabay, Unsplash, Wikipedia, AdobeStock